



Council of European National
Top-Level Domain Registries



IETF 123

The **123rd IETF meeting** was held in Madrid, Spain, from 19 to 25 July 2025, featuring over **190** working group sessions, a two-day hackathon, and numerous side events. Pawel Kowalik and Christian Simmen from DENIC attended and have prepared a summary highlighting the key points relevant to CENTR members.

PAWEL KOWALIK & CHRISTIAN SIMMEN, DENIC EG





Table of contents

Introduction **3**

Informal activities **3**

Hackathon	3
RESTful Provisioning Protocol (RPP)	3
DNS Projects	4
Post-Quantum Cryptography Activities	4
IEPG	4

Side Meetings **5**

AoT/ADoQ Deployment Initiative	5
PQ DNSSEC	5
Evaluating PQC in DNSSEC Signing for TLD Operators	6
Impact of Merkle Tree Ladder Mode Signatures on DNSSEC	6
A Deeper Look: Merkle Tree Ladder Mode	7
Proposed Strategy and Community Feedback	7

Formal Proceedings **8**

DNSOP WG	8
DELEG WG	10
REGEXT WG	11
RPP WG	12

Epilogue **14**

Introduction

The mission of the Internet Engineering Task Force (IETF) is to improve the internet. While most of the IETF's work is conducted online, the organisation also holds three meetings each year. The 123rd IETF meeting was held in Madrid, Spain, from 19 to 25 July 2025.

With **1,738 registered participants**, this was the best-attended meeting since IETF 118 in Prague. Around two-thirds of participants (1,097 or 63%) were present on site, with the remainder joining remotely via the Meetecho platform.

The **IETF Hackathon**, held on the weekend before the main sessions, had 682 registered participants (597 on site, 85 remote), working on over 60 different projects. There was also a '**code sprint**', at which a small group of volunteers worked at improving the tools made available by the IETF, such as the well-known **Datatracker**.

Every IETF meeting offers a **packed programme**. The latest week-long gathering featured over 190 working group sessions, the IEPG meeting, HotRFC Lightning Talks, a **plenary session**, and a wide variety of side meetings.

Informal activities

During the weekend prior to the main meeting, there were various informal activities: a Hackathon, the IEPG, and the HotRFC Lightning Talks.

Hackathon

The now traditional Hackathon got under way on the Saturday prior to the main proceedings. At the Hackathon, the applicability and interoperability of new concepts were tested on a collaborative, non-competitive basis. Groups were formed spontaneously to work on a **range of experiments** from a list of 36 projects. A total of 476 participants interacted and programmed together intensively throughout the weekend. The Hackathon concluded with result **presentations**.

RESTful Provisioning Protocol (RPP)

The **RPP hackathon** continued to prototype an alternative to EPP for domain name provisioning. The team worked on experimental implementations of the RPP core protocol and explored alternative representations for DNS data.

The effort was highly productive, yielding five working implementations, three of which were linked to real registry systems (DENIC, Afnic, SIDN). Participants tested both native RPP deployments and RPP-to-EPP proxy models. Key outcomes included aligning the draft URL structure, proposing methods for handling EPP authorisation codes, and using Problem Detail documents for error responses. Future work will focus on creating a publicly available test environment and finalising the API and data model specifications.

DNS Projects

Traditionally the “DNS table” was full of projects focused on DNS operations and performance. Among others the following implementations shall gain attention:

- Generalised NOTIFY: A Python implementation was created for the now-finalised [draft-ietf-dnsop-generalized-notify](#) to generate and dispatch NOTIFY messages for CDS and CDNSKEY records.
- **Opportunistic Transport signalling**: Work was done on an experimental resolver and authoritative server to support signalling for transports like DoT, DoQ, and DoH, allowing servers to announce support for secure transports.

Post-Quantum Cryptography Activities

Continuing the momentum from IETF 122, there was considerable activity around post-quantum cryptography. The “PQC DNSSEC Algorithms and Non-Existence Responses” project examined the impact of PQC on DNSSEC, with a particular focus on NSEC/NSEC3 responses and the performance of new algorithms. This work built on earlier hackathon initiatives to test PQC implementations in DNSSEC and collect meaningful performance metrics.

IEPG

The Sunday morning of an IETF meeting traditionally begins with the **IEPG** (Internet Engineering and Planning Group), where attention is focused on **topics** with some form of operational significance.

Presentations at IETF 123 included:

- **Alex Huang Feng** – Detecting External Disruptions in Internet Services Provider Networks
- **Geoff Huston** – QUIC Safari, HTTPS and the DNS
- **Jeff Haas** – BGP path attribute filtering impacts

Side Meetings

Side meetings are held alongside the official IETF agenda and often provide an opportunity to discuss emerging issues that the technical community may need to address in the near future. At times these meetings lead to the creation of official working groups, while in other cases they simply serve as a forum for collaboration and the exchange of information.

AoT/ADoQ Deployment Initiative

The meeting brought together operators and vendors to advance the adoption of encrypted DNS between recursive and authoritative servers. Chaired by Sara and John Dickinson, the session attracted around 50 participants on site and 60 online, who shared experiences, outlined future plans, and explored opportunities for collaboration. Its primary aim was to address the slow roll-out of Authenticated DNS over TLS (ADoT) and QUIC (ADoQ) by establishing a forum for stakeholders to coordinate their efforts.

The discussion highlighted several key challenges, most notably the classic “chicken-and-egg problem”: recursive resolvers are reluctant to enable encryption if few authoritative servers support it, and vice versa. Performance was another significant concern, with some operators noting that DoT can be an order of magnitude slower than unencrypted UDP. Nevertheless, there was strong consensus that QUIC represents the more promising long-term solution, offering superior performance characteristics. Demand, however, remains fragmented: while some operators see interest driven by business requirements and regulatory frameworks, others report that most enterprise customers are not yet requesting this feature.

To break the deadlock, two key paths forward were identified. As a pragmatic short-term solution, a public JSON list of authoritative servers that support encrypted transports was proposed, allowing resolvers to begin using them immediately without waiting for new standards. For a mid-term, standards-based approach, a [draft that uses SVCB records](#) for opportunistic signalling of supported transports was presented, whereas DELEG would likely be the ultimate long-term approach. The initiative will continue to provide a venue for operators to share performance data and collaborate on these solutions, with the hope that emerging EU regulations like NIS2 may also serve as a catalyst for wider adoption.

PQ DNSSEC

With multiple regulatory bodies setting deadlines as early as 2030 for the adoption of post-quantum technologies in critical systems, the DNS community is actively exploring potential paths for DNSSEC development. The session included three presentations—from SIDN Labs, NLnet Labs, and Verisign—covering evaluations of new post-quantum cryptography (PQC) algorithms, the effects of mitigation techniques such as Merkle Tree Ladder (MTL) Mode, and a proposed strategy for the transition.

Evaluating PQC (Falcon and Mayo) in DNSSEC Signing for TLD Operators

Elmer Lastdrager of SIDN Labs presented an [evaluation of the PQC algorithms Falcon-512 and MAYO-2](#) against traditional RSA and ECDSA for DNSSEC signing in Top-Level Domains (TLDs). The study tested the algorithms on the .nl, .se, and .nu zone files.

Key findings included:

- **Signature and Key Sizes:** Falcon-512 produces a 666-byte signature, whereas MAYO-2 has a smaller 180-byte signature but a much larger public key (5,488 bytes vs. 897 bytes for Falcon).
- **Impact on Zone Size:** The larger keys and signatures significantly increase the size of signed zones. For the ~1 GB unsigned .nl zone, signing with Falcon-512 expanded it to ~12 GB, while MAYO-2 resulted in ~5 GB. This is considerably larger than RSA (~4.5 GB) and ECDSA (~3 GB).
- **Performance:** On modern x86-64-v3 hardware, signing with MAYO-2 was roughly 1.3× slower than the baseline, while Falcon-512 was about 2.1× slower. For validation, Falcon was approximately 1.3× slower than the baseline, whereas MAYO-2 achieved 0.7× of the baseline—comparable to ECDSA.

Impact of Merkle Tree Ladder (MTL) Mode Signatures on DNSSEC

Willem Toorop of NLnet Labs presented work by Jannik Peters on the [impact of using SLH-DSA with Merkle Tree Ladder \(MTL\) Mode in DNSSEC](#). This approach aims to mitigate the large signature sizes of PQC algorithms.

Key findings included:

- **Signature Size:** MTL mode dramatically reduces the signature size for most DNS records to a “condensed” format of 40–500 bytes, easily fitting within UDP packets. However, SOA and DNSKEY records still require a “full” signature exceeding 8 KB. Since NXDOMAIN and NODATA responses include the SOA record, they also require large signatures, which would necessitate a switch to TCP.
- **Performance:** MTL mode makes the otherwise slow SLH-DSA algorithm competitive in both signing and verification. Signing a zone with SLH-DSA-MTL takes 600–900 ms, compared to 358 ms for ECDSA—orders of magnitude faster than non-MTL SLH-DSA.

Table II
DNS Message Size (root zone with 1 KSK and 1 ZSK)

Algorithm	SOA	DNSKEY	NXDOMAIN	NODATA	Delegation
ECDSAP256SHA256	197	280	319	316	333
SLH-DSA-MTL-SHA2-128s	8366	8089	8641	8638	486
SLH-DSA-MTL-SHAKE-128s	8366	8089	8641	8638	486
SLH-DSA-SHA2-128s [†]	7989	8072	15903	15900	8125
SLH-DSA-SHAKE-128s [†]	7989	8072	15903	15900	8125

[†] Estimated message sizes, calculated by hand.

Queries: . IN {NS,SOA,DNSKEY} - . IN A (NODATA) - aa. IN A (NXDOMAIN)

Figure 1 Calculated message sizes compared between MTL and non-MTL variants

A Deeper Look: Merkle Tree Ladder (MTL) Mode

Merkle Tree Ladder (MTL) Mode is a technique designed to reduce the operational impact of large signatures in protocols like DNSSEC. Instead of signing each DNS RRset individually, a single signature is created for a structure called a Merkle Tree Ladder, derived from all RRsets in a zone. Each RRset is hashed to form a “leaf” in a binary tree. These hashes are combined upward, with each parent node representing the hash of its children, until a single “root” hash, or rung, is produced for the tree.

The ladder—the object that is actually signed—consists of a collection of these rungs. To authenticate a specific RRset, a resolver receives a small condensed signature containing an authentication path: the set of sibling hashes needed to recalculate the root rung from the RRset. The resolver then verifies the RRset’s authenticity by confirming that the recalculated rung is included in the signed ladder.

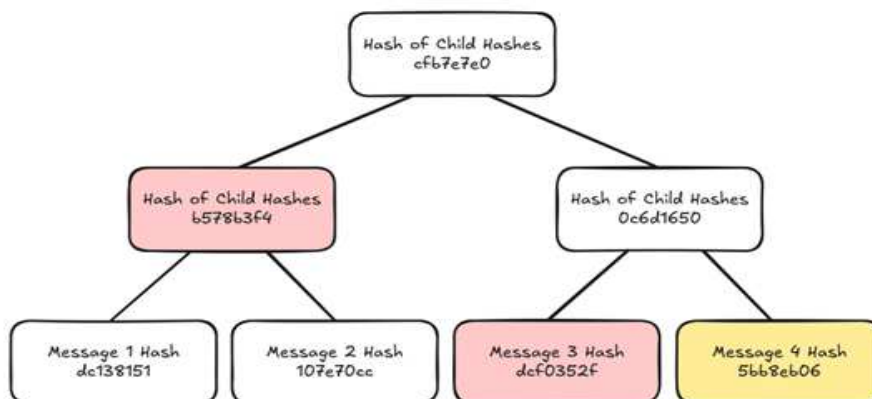


Figure 2 Example authentication path in MTL Mode

Proposed Strategy and Community Feedback

Joe Harvey of Verisign outlined a post-quantum strategy for DNSSEC, stressing the urgency of taking action before NIST finalizes its next set of PQC algorithms, especially given impending

deadlines for phasing out RSA and ECDSA. At the heart of his proposal is a “diversity strategy” for DNSSEC, designed to avoid dependence on any single cryptographic assumption.

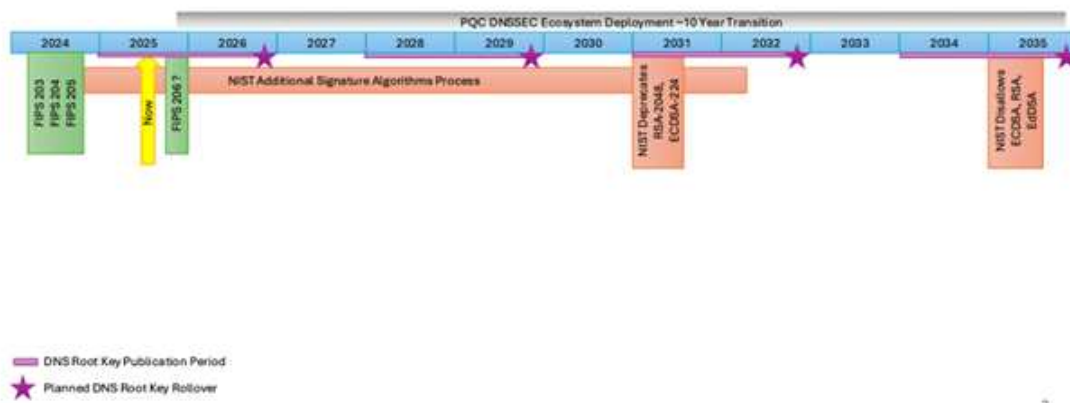


Figure 3 DNSSEC Cryptography Deployment Lifecycles

The proposed strategy includes:

- Deploying multiple PQC algorithms: At least two types would be used—one conservatively designed algorithm for resilient fallback, and one low-impact, drop-in algorithm for routine performance.
- Algorithm selection: SLH-DSA is suggested as the conservative “resilient fallback” option, while no recommendation has yet been made for the low-impact algorithm.
- Operator flexibility: DNS operators would have the freedom to choose which algorithm to deploy for their zones.

Next steps involve continuing community discussions to identify a suitable low-impact algorithm and analysing potential resource-consumption attacks.

Formal Proceedings

A selection of working group sessions is outlined below. Since many sessions run in parallel, choosing which to attend can be challenging. This list does not cover every topic from all working groups; rather, it reflects the author’s selection of sessions most relevant to the CENTR community.

DNSOP WG

As always, the DNSOP Working Group, which is concerned with the evolution of (the operational aspects of) the DNS protocol, was very active and its sessions were well attended. A few highlights are presented below. For a list of all discussed drafts can be found on the [meeting agenda](#).

Published Work

No new RFCs were published since the previous IETF meeting.

Work in Progress

- [draft-ietf-dnsop-domain-verification-techniques](#) was presented by Erik Nygren. This draft elaborates on DNS based ownership validation techniques (“Domain Control Validation”). For example, these are requested by Certificate Authorities when issuing TLS certificates to prove control over the domain the certificate is requested for. Unlike [ACME \(RFC8555\)](#) this draft aims for a broader range of use cases.
- [draft-ietf-dnsop-structured-dns-error](#) was presented by Tiru Reddy. This document was sent back to the working group to potentially include [draft-nottingham-public-resolver-errors](#). Both documents aim to signal more detailed information in case DNS filtering has happened. Draft-ietf-dnsop-structured-dns-error makes use of the Extended DNS Errors (EDE, RFC 8914) “EXTRA-TEXT” field to store a JSON structure containing justification and contact information of the filtering organization. Draft-nottingham-public-resolver-errors enhances this structure by adding DNS Filtering Database Entries to further enhance transparency.
- Tobias Fiebig presented on measurements of DNS resolution comparing IPV4 and IPV6 transport. [draft-ietf-dnsop-3901bis](#) documents Best Current Practice for operating authoritative DNS servers as well as recursive and stub DNS resolvers.

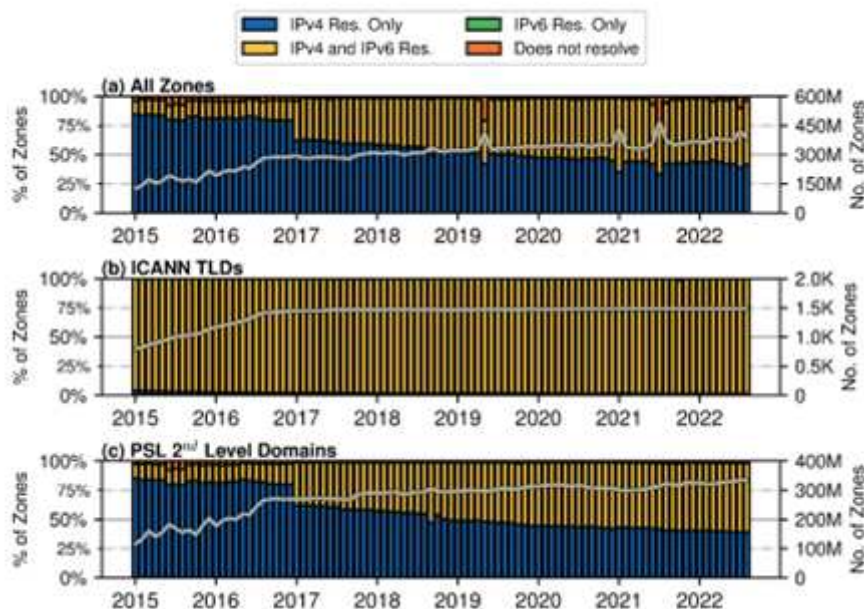


Figure 4 IPv6 adoption in DNS

Potential New Work

- [draft-shetho-dnsop-ds-automation](#) was presented by Peter Thomassen. Parent zone operators deploying DS automation systems have to make a number of decisions regarding validity checks, timing, error reporting, security and locking mechanisms. The draft gives

recommendations to be considered in these deployments.

- Shumon Huque presented [draft-huque-dnsop-multi-alg-rules](#). Multisigner setups, especially when operated by different providers, face operational problems when it is intended to also have different signing algorithms or in case of an algorithm rollover. The draft makes adjustments to the requirements on DNSSEC signing and validation.
- [draft-berra-dnsop-announce-scanner](#) was presented by Johan Stenstam. The draft enhances transparency for child zone operators by allowing parent zone operators to state the presence or absence of a CDS or CSYNC scanner. Deriving from generalized notifications draft it is also possible to instruct child zone operators where to send notifications to have a scanner to take an immediate look at the child (e.g. in case the CDS may have changed).

DELEG WG

The DELEG Working Group is developing a new DNS signalling mechanism to solve operational problems that arise from the limited ability of parent servers to provide additional information about child delegations.

Work in Progress

David Lawrence presented the changes made to [draft-ietf-deleg](#). Improvements were made to resiliency against downgrade attacks and error behaviour.

Currently DELEG supports two types of delegation. “DELEG DIRECT” is used if the target of the delegation is below the delegated domain and contains a target name and optional GLUE IPs. “DELEG INCLUDE” is used if the target is outside the delegated domain finally targeting a SVCB record. In this case - just like for NS records - no GLUE is needed.

```
example. 300 IN DELEG DIRECT a.example. Glue4=192.0.2.1 (  
Glue6=2001:DB8::1 )
```

```
example. 300 IN DELEG INCLUDE ns2.example.net.
```

An idea was discussed to omit the target name for “DELEG DIRECT”. Paul Hoffman gave an overview of the advantages and disadvantages of this “[nameless delegation](#)”

The reuse of SVCB records as target record type for DELEG INCLUDE is still an [active discussion](#). SVCB has the benefit of sharing DELEG record format and being recognized by DNS software. However slight differences from SVCB to DELEG would also apply here. Creating a new record type could be more tailored to the needs, but comes at the cost of additional complexity.

REGEXT WG

The REGEXT (Registry Extensibility) working group focuses on coordinating and developing standard extensions for key Internet registry protocols. Its main role is to manage the standardization of extensions to the Extensible Provisioning Protocol (EPP), used for domain name registration, and the Registration Data Access Protocol (RDAP), used to access registration data.

Published Work

[RFC 9803](#) - EPP Mapping for DNS Time-To-Live (TTL) Values

This extension enables clients to modify the TTL of their domain's delegation records, including NS, DS, A, and AAAA records. It is especially useful for speeding up operational changes, such as migrating to new DNS servers or performing DNSSEC key rollovers.

Work in Progress

Updates were provided on several ongoing drafts.

Work on [versioning in RDAP](#) is continuing, with a recent clarity updates made to the draft and a call for more implementation experience before it moves forward.

The draft for [using JSContact in RDAP JSON Responses](#), which defines a richer format for contact information, has been moved to “Experimental” status. Mario Loffredo noted that recent updates incorporated the new JSContact profiles specification, which helped reduce the set of required properties.

The working group spent also time discussing a [draft on guidelines for extending RDAP protocol](#). The document aims to offer clarity for all extension authors to keep interoperability of the whole protocol and avoid potential conflicts. One aspect where the participants were still looking for consensus was how the identifiers should be structured. This aspect will be further discussed on working group [mailing list](#) with a clear [call for more voices to weight in](#).

Potential New Work

The session included presentations on several proposals for new work within the working group.

Domain Variant Support for EPP

The [extension](#) proposed by James Galvin is designed to manage a set of related domain variants as a single group, where the entire group's lifecycle is tied to a designated “primary” label. Key open issues being discussed include changing the terminology from “variant” to “related group” to better accommodate things like Latin diacritics. The authors requested that the working group adopt the draft.

Domain Registry Grace Period Mapping for EPP

A [draft to update the Registry Grace Period \(RGP\) mapping \(RFC 3915\)](#) was presented by Rick Wilhelm on behalf of the authors. The presenters clarified that the work's sole purpose is to fix a bug identified in the original RFC. The issue is a mismatch between the RFC's narrative text, which states only a single <rgp:status> element is allowed, and the XML schema, which allows for an unbounded number. This discrepancy could cause clients that only expect a single status to process responses incorrectly. A concern was expressed that even with this minor correction the change of the namespace version to urn:ietf:params:xml:ns:epp:rgp-1.1 will cause migration impact, which may be an opportunity to make more changes to the process, like replacing 2-step restore process with one step or adding structured end date to the status.

RDAP Extension for Verified Contact Information

Mario Loffredo presented a [proposal for an RDAP extension](#) to signal the verification status of contact information. This extension would allow RDAP responses to explicitly show whether contact details like email, phone numbers, or postal addresses have been verified. This work is directly relevant to regulatory requirements, such as Article 28 of the EU's NIS2 Directive, which mandates that registries and registrars verify the accuracy of registration data. The proposed mechanism involves adding a new element to the RDAP entity response, which would contain the verification date and the method used. The proposal was met with positive feedback in the session.

RPP WG

The RESTful Provisioning Protocol (RPP) Working Group is developing a standardized protocol for domain name management between registries and registrars, offering a modern REST- and JSON-based alternative to the existing Extensible Provisioning Protocol (EPP).

The focus of the working group is to find consensus on the [requirements](#). This milestone is expected to be reached at [IETF 124](#) meeting in November. All milestones - and other necessary information to participate - can be found on the [working group page](#) in the IETF datatracker.

Work in Progress

An overview of [RPP design challenges](#) has been given by Pawel Kowalik. These include the HTTP verbs used for object creation, design of the EPP CHECK command, design of processes associated to objects (e.g. transferring an object), authcode handling and the design of optional properties.

James Gould presented the current status of the [EPP extension analysis](#). 65 extensions were analyzed and categorized in four categories:

- **Embed:** These EPP extensions should be included in the core documents.
- **Extension:** An RPP extension should be defined.

- **Design:** RPP should be designed in a way that an extension could be created.
- **not applicable:** no actions taken for RPP

The full analysis and recommendations can be found in this [Google Doc](#).

Maarten Wullink raised some questions for an [in-depth discussion about the requirements](#) for RPP. These questions have also been asked to the CENTR community at the last Jamboree. Notes on the discussion and results of the polls can be found in the [meeting minutes](#).

Potential New Work

Pawel Kowalik presented his draft of the RPP architecture ([draft-kowalik-rpp-architecture](#)). The draft describes the architectural principles of RPP:

- HTTP and RESTful principles are foundational
- A resource-oriented architecture
- Domain-specific logic resides in data representations
- Layered architecture for modularity

The draft has been reviewed and is recommended for working group adoption.

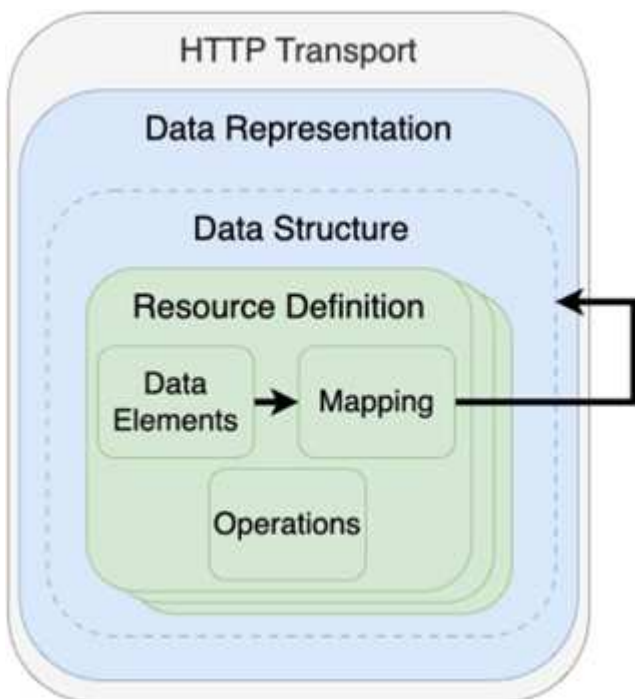


Figure 5 Layers in RPP

Christian Simmen gave an [introduction](#) for a unified, extensible JSON representation for DNS resource records. [draft-simmen-rpp-dns-data](#) aims for a closer alignment of the provisioning format of DNS data in RPP to the target system by mapping DNS resource records into a JSON structure which can be used for host attributes, host objects and other objects containing DNS data.

Epilogue

IETF 123 was another successful meeting, and the hosts and sponsors deserve congratulations. The program was full and engaging, offering ample opportunities for networking. Both IETF and IRTF working groups maintained a strong focus on the future, making the meeting consistently stimulating and relevant.

The **next IETF meeting** is scheduled for 1 – 7 November 2025 in Montreal.



**Council of European National
Top-Level Domain Registries**



About CENTR


CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 51 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide.

The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries.

Full membership is open to organisations, corporate bodies or individuals that operate a country code top level domain registry.

CONTACT

 **CENTR VZW/ASBL**
Belliardstraat 20
1040 Brussels, Belgium
0885.419.166 | RPR Brussels

 +32 2 627 5550

 secretariat@centr.org

 www.centr.org

FOLLOW US

To keep up-to-date with CENTR activities and reports, follow us on Twitter or LinkedIn



© This publication has been authored by CENTR. Reproduction of the texts of this publication is authorised, provided the source is acknowledged.